REMARKS/ARGUMENTS

Claims 1, 2, 5 and 6 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (U.S. Pat. No. 6,182,214) in view of Bellare et al. (Proposal for P1363 Study Group on Password-Based Authenticated-Key-Exchange Methods). Claim 3 was rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono in view of Newton (U.S. Pat. No. 5,771,291). Claims 4 and 7 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono in view of Denning (Descriptions of Key Escrow Systems).

Applicants respectfully traverse the rejection of claims 1-4. Claims 1-4 recite in part "at least one secret value including a master key, the master key being split into two or more parts wherein fewer than all the parts are required for reassembling the master key, **the parts being encrypted by a password-derived or token-based key, each part being associated with a password wherein the at least one server can update the master key by requiring only some of the passwords to be revealed**" (emphasis added). At page 3, paragraph 4 b. of the office action it is stated that the Hardjono reference teaches this claim limitation. Applicants fail to find any teaching or suggestion for this limitation in Hardjono. Hardjono is simply concerned with sending a secret over an unreliable network to one or more clients. Hardjono uses threshold cryptography (secret sharing) to overcome the problems of the unreliable network. Hardjono's server transmits N shares to the client spreading the N shares over a number of transmitted messages, with the assumption that the client will correctly receive some of the messages, including at least M shares (see col. 3, 49-56). There is simply no teaching or suggestion in Hardjono or in Bellare et al. (or any of the other cited references) taken individually or in combination on how to update a master key by a server as recited in claims 1-4. There is no discussion in the references on how a master key can be modified by a server by requiring only some passwords to be revealed. Neither of the cited references, address the issue being addressed by the claims on how to update a

master key by a server (see page 9, lines 21 to page 10, line 8 of the present application). As such, it is believed that claims 1-4 are in condition for allowance.

Claims 5 and 6 have been amended to clarify the claim language. As amended claims 5-7, claim in part "encrypting the parts by a password-derived or token-based key, each part being associated with a password, wherein the master key can be reassembled by the server by requiring only some of the passwords to be revealed." Like previously discussed above neither the Hardjono or Bellare et al. reference (or any of the other references), teach or suggest reassembling a master key by a server by requiring only some of the passwords to be reveled. As such, it is believed that claims 5-7 are also in condition for allowance.

New claims 8-10 have been introduced; no new matter has been added. New claims 8-10 are also believed to be in condition for allowance given the comments made above.

Applicants respectfully request reconsideration and allowance of the pending claims. If the Examiner feels that a telephone conference would expedite the resolution of this case, he is respectfully requested to contact the undersigned.

In the course of the foregoing discussions, Applicants may have at times referred to claim limitations in shorthand fashion, or may have focused on a particular claim element. This discussion should not be interpreted to mean that the other limitations can be ignored or dismissed. The claims must be viewed as a whole, and each limitation of the claims must be considered when determining the patentability of the claims. Moreover, it should be understood that there may be other distinctions between the claims and the cited art which have yet to be raised, but which may be raised in the future.

Applicants respectfully request that a timely Notice of Allowance be issued in this case. If any fees or time extensions are inadvertently omitted or if any fees

have been overpaid, please appropriately charge or credit those fees to Hewlett-Packard Company Deposit Account Number 08-2025 and enter any time extension(s) necessary to prevent this case from being abandoned.

Respectfully submitted,

Pedro P. Hernandez
PTO Reg. No. 35,190
CONLEY ROSE, P.C.
(972) 731-2288 (Phone)
(972) 731-2289 (Fax)
ATTORNEY FOR APPLICANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Fort Collins, CO 80527-2400